THOMPSON COBURN LLP

One US Bank Plaza
St. Louis, Missouri 63101
314-552-6000
FAX 314-552-7000
www.thompsoncoburn.com

January 28, 2011

Mark Sableman
314-552-6103
FAX 314-552-7103
msableman@
thompsoncoburn.com

By PDF email to privacynoi2010@ntia.doc.gov

Internet Policy Task Force
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Re: Comments on *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (the "Report")

Dear Internet Policy Task Force:

These comments are submitted on behalf of American Business Media ("ABM"), an association representing more than 200 business-to-business information providers, including print and digital publishers, websites, and organizers of trade shows and similar events. Producing hundreds of high-quality business-to-business publications, ABM members play an essential role in assembling and disseminating the industry-specific news and information needed by businesses and key industries in thousands of different fields worldwide.

Summary of Comments

ABM's comments focus on the implications of the issues and recommendations in the Report on business-to-business ("B-to-B") communications, the area in which most of its members focus their activities. B-to-B generally refers to communications or transactions between businesses, such as between a manufacturer and a wholesaler, or between a wholesaler and a retailer, and especially communications between and among businesses conducted through trade journals and websites—the latter being the core of ABM members' businesses. ABM believes that the unique nature of B-to-B communications and transactions need to be considered in connection with policy making concerning data privacy. Indeed, courts have long recognized that neither business entities nor the individuals who act on their behalf have personal privacy rights in their business activities.

ABM agrees with the many comments in the Report that support industry self-regulation as the best way to address data privacy concerns, particularly with respect to new and emerging technologies. ABM appreciates the department's support for the self-regulation process, and believes that self-regulation programs in the data privacy area must be given room to develop.

Indeed, ABM believes that promulgating any new statute or legally required guidelines is likely to chill growing commerce in the Internet environment.

In these comments, ABM addresses the following issues set forth in Appendix A to the Report: (1&2) Fair Information Practice Principles, (3) voluntary codes of conduct and safe harbors, (4) the proposed Privacy Policy Office, and (6) global harmonization.

Background: Business-to-Business Communications and Transactions

ABM members chiefly deal with business entities and their personnel concerning business-related matters. It has been estimated that the B-to-B industry in the United States publishes approximately 2,000 B-to-B magazines and approximately 3,500 websites. ABM members include many of the largest and best-known publishers of such magazines and websites, including, for example, Crain Communications, publisher of *Advertising Age*, and The McGraw-Hill Companies, publisher of *Engineering News-Record* and *Dodge Reports*.

B-to-B communications have long played a crucial role in our economy in providing information to the business community and in making connections among businesspeople, thereby fostering commerce and economic growth, including e-commerce. ABM members' online and offline content, trade shows and events are essential to the growth and vibrancy of United States businesses. The products and services produced by our members, both content and advertising based, are essential to businesses, their owners and their employees and contractors throughout the world, greatly enhancing their ability to obtain important technical, market and industry information that allows them to prosper.

Like other information providers, ABM members have increasingly turned to digital methods of publishing and distribution. This medium enables them to communicate quickly and effectively with their subscribers and constituents, and provides other benefits as well, including the ability to tailor information and advertising to business users' particular needs, interests and even geographic location.

In addition to their print and digital activities, many ABM members produce trade shows and events, including online informational seminars and webcasts, spanning both geographic regions and industry sectors. Such events promote commercial activity, by bringing business buyers and sellers together, allowing them particularly to obtain and share information, best practices and business contacts.

Business-to-business information providers conduct data collection and use involving different kinds of data, including, for example, technical data, industry metrics and analyses, government reports, in order to assist their business customers in their decision-making. To the extent B-to-B data collection activities include data about individuals, such information usually relates to those individuals in their *business capacities*—that is, information obtained about an individual in his or her role as an employee or representative of a business enterprise (which may include for-profit businesses, associations, non-profit entities, and other

organizations). For example, a typical piece of B-to-B data about an individual may consist of a name, job title, business name, business contact information, and particular business interest—all quite different from the data concerning individuals in their private capacities that are usually the subject of consumer privacy discussions.

Like all business entities, ABM members are subject to laws of general application, such as section 5 of the FTC Act, and to various self-regulatory and prudential business practices, such as adherence to codes of conduct and to the expectations of business users. In general, as the comments below explain in more detail, ABM believes that imposition of new regulations on providers of B-to-B information, particularly regulations written with a view to perceived problems in business-to-consumer transactions, could improperly inhibit or restrict valuable and unique B-to-B activity.

In the specific comments below, ABM responds to certain of the Recommendations and Questions for Further Discussion set forth in Appendix A to the Report. Our responses are referenced according to the numbering used in Appendix A.

Commerce Issue #3 – Encouragement of Voluntary Codes of Conduct; Safe Harbors

ABM strongly supports actions that encourage the development of voluntary codes of conduct and industry self-regulation procedures. As the Report notes, the self-regulatory framework developed by the advertising industry for online behavioral advertising covers a "sophisticated" technology, yet is providing "sensible protections for consumers," while maintaining the flexibility necessary for such an emerging technology, as the program "continues to be updated" to meet new challenges. (Report, page 42.)

Broad prescriptive rules developed by government agencies, even when framed as "principles," often lack the flexibility, practicality and workability of voluntary industry codes and procedures, particularly in the areas of new technologies. Accordingly, ABM strongly supports the development and encouragement of such codes and procedures by industry that may also require some governmental forbearance from imposition of rigid rules or principles, particularly as new technologies and methods emerge. ABM notes, moreover, that the online behavioral advertising self-regulatory program that the Report correctly praises came together without any governmental participation.

ABM also supports the concept that the government should recognize a safe harbor for industry actions made in compliance with recognized and approved self-regulatory standards. ABM believes that compliance with the carefully developed self-regulatory program with respect to online behavioral advertising should qualify a participant for a safe harbor.

Commerce Issues #1 and #2 – Fair Information Practice Principles (FIPPs)

ABM supports the use of Fair Information Practice Principles (FIPPs) solely as a privacy framework and self-regulatory baseline, to assist companies in analyzing and strengthening

customer privacy practices, but not as formally codified and rigid rules. B-to-B information providers believe that formal codification of baseline FIPPs would interfere with the flexibility and nimbleness needed for continued online innovation.

From the experiences of ABM member companies, we know that development of Fair Information Practice Principles (FIPPs), like development of privacy laws and regulations, and industry self-regulation principles, can be complex and involve resolution of many different competing interests, as well as factual and technological issues. However, industry has been adept at developing and adapting such systems to the realities of the marketplace and is concerned that imposition of theoretical privacy principles could create many problems themselves, particularly if the principles are not developed with full participation from all interested groups, and full understanding of empirical realities.

In particular, ABM opposes as unnecessary and counterproductive a new baseline privacy statute. New rules, whether framed as specific commands or as general principles, would be inherently rigid and would inhibit business and innovation. ABM believes that one-size-fits-all information practice principles cannot be written without interfering with important aspects of commerce, including the business-to-business communications and transactions engaged in by ABM members.

There are significantly different interests involved in collection, use and transfer of information about individuals in their private capacities, and about individuals in their business capacities. Specifically, FIPPs designed to protect consumer privacy should not cover collection and use of information obtained in a person's *business capacity*—that is, information obtained about an individual in his or her capacity as an employee or representative of a business enterprise (which may include for-profit businesses, associations, non-profit entities, and other organizations).

Importantly, courts have recognized the distinction between business users and individuals acting in their personal capacities, with respect to privacy interests. Initially, it is well-recognized that neither business entities nor the individuals who act on their behalf have personal privacy rights in their business activities. "[C]orporations can claim no equality with individuals in the enjoyment of a right to privacy." *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950); *see also* Restatement (Second) of Torts § 652I cmt. c ("A corporation, partnership or unincorporated association has no personal right of privacy."); *Browning-Ferris Indus. v. Kelco Disposal, Inc.*, 492 U.S. 257, 284 (1989) (O'Connor, J., concurring in part, dissenting in part) ("[A] corporation has no ... right to privacy."). Indeed, the Supreme Court has recognized that "a business, by its special nature and voluntary existence, may open itself to intrusions that would not be permissible in a purely private context." *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 353 (1977). Many courts have found that business employees, acting as such, have little or no privacy interests in their business conduct. *E.g., Curto v. Medical World Communications, Inc.*, 2006 WL 1318387 (E.D.N.Y. 2006) ("Employees expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network.").

Subjecting communications with persons in their business capacities to the same limits, rules and practice principles as apply to communications with persons in their personal capacities, especially if those rules or principles involve what are essentially opt-in requirements for collection and sharing of information, would significantly hamper the flow of business information and subsequently the flow of commerce crucial to America's economic growth and prosperity.

Moreover, data privacy issues that may arise in the course of business-to-business communications and transactions are generally addressed through notice-and-choice safeguards and industry codes and customs that have developed over time, based on the needs of the business community and the pressures of the competitive marketplace. Just as the business marketplace demands that businesses take care in protecting trade secrets and other confidential information when sharing or use of such information is required, that marketplace ensures that notice-and-choice procedures and other means protect data privacy as appropriate. These are further reasons why there is no need for government to intervene and prescribe new rules in this area.

We also urge the Department to consider the unique privacy implications that must be considered with in the context of offline collection of basic information from persons acting in clear business capacities. Especially as to *offline* collection of information, the capacity of an individual (whether he or she is acting in a professional capacity or a personal capacity) can be easily determined. While it is slightly more difficult to distinguish business and personal capacities *online*, the context in which information is collected or used usually clarifies this. For example, someone who shops at Macy's online should be presumed to be acting in a personal capacity, but someone who visits the *Engineering News-Record* website should be presumed to be acting in a business capacity—or at least, to be knowingly seeking business information, and protected by the ability to opt-out of any information collection and use in which he or she does not wish to participate. That is, much different privacy protections are appropriate for business-focused websites and contexts than for consumer websites and contexts.[1]

In addition to recognizing excluding coverage for B-to-B communications, ABM believes that in formulating FIPPs, the Department should provide that certain other areas, briefly outlined below, fall outside of their coverage, or otherwise provide room for these practices to continue using customary privacy safeguards such as notice and choice procedures.

[1] The context and business nature of a website, trade show, or other place where B-to-B communications occur should be the guidepost for distinguishing between B-to-B and business-to-consumer communications and transactions. That distinction should *not* be based on whether a home or office address is used, since in many fields of business, home addresses are often used for business purposes.

Contextual advertising. "Contextual advertising" refers to advertising based on a consumer's current visit to a single web page or a single search query that involves no retention of data about the consumer's online activities beyond that necessary for the immediate delivery of an ad or search result. ABM agrees with the Federal Trade Commission staff that contextual advertising should fall outside any new data privacy regulations. FTC, *Protecting Consumer Privacy in an Era of Rapid Change* [hereafter, "*2010 FTC Report*"], Dec. 2010, p. 55 n.134.

First Party Marketing. ABM believes that where information is collected by a trusted first party, it should be sufficient for that party to give traditional notice and choice as to its practices in sharing that information. Users who seek out a particular first-party website do so because they trust the first party and the disclosures and promises that the first party has made. Users who voluntarily provide information to the first party do so with full knowledge of the first party's disclosed information use practices, no additional required disclosures or regulatory interventions are necessary. As recognized in the FTC's February 2009 privacy report, "first party" behavioral advertising practices "are more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than practices involving the sharing of data with third parties or across multiple websites" and accordingly do not need to be regulated. FTC, *Self–Regulatory Principles for Online Behavioral Advertising*, Feb. 2009 at pages 26-28.

Data Sharing Among Affiliates. All marketing by business units under common control or close affiliation should be treated as first-party marketing. Just as first parties are trusted, their business affiliates are trusted as well, and businesses take care that all affiliates operate in a manner that reflects and supports of the strength of their brands' integrity in the marketplace. When someone gives information to a particular business, he or she understands that the information is available for use not only for a particular business unit, but for all business units under common control and ownership or close affiliation. At least in connection with business communications, all marketing within commonly owned or controlled or affiliated companies should be recognized as first party marketing.

Third Party Marketing. Under current practices, when first parties collect information that may be shared with third parties, they provide notice to their users of their information-sharing practices, and provide means by which the users may opt out of such sharing (which may, in some cases, require the users to forebear from sharing their information with the first party in the first place). This well-established notice-and-choice practice works well and should not be disturbed. More restrictive rules with respect to information sharing with third parties would prevent or inhibit many useful business practices, particularly in the B-to-B marketplace, including information sharing at trade shows, and customary business list rentals.

Legal compliance. Information content businesses often must collect data about their users in order to track compliance with legal requirements such as licensing

> restrictions, and in order to prevent copyright infringement or piracy. As the *2010 FTC Report* notes (pages 54-55), in any data privacy regulations, care must be taken to exempt customary data collection measures designed for such purposes and for other necessary purposes, such as product and service fulfillment.

Thus, at the very least, if FIPPs are developed, they should not cover collection, use and transfer of information in B-to-B communications and transactions, or they should be carefully tailored to distinguish between collection of information about individuals in their individual capacities and about them in their business capacities. They should also not cover the other necessary and proper practices outlined above.

Finally, ABM believes it is premature to comment on particular FIPPs issues, because development of specific FIPPs will require careful study of empirical data concerning both privacy needs and particular ways of meeting those needs. In any event, if and when FIPPs are developed, the involvement and input of the B-to-B community should be sought at every step in the process.

Commerce Issue #4 -- Establishment of a Privacy Policy Office

ABM would support creation of a Privacy Policy Office only to the extent it would bring stakeholders together towards voluntary codes of conduct and best practices. However, ABM believes that if Commerce creates such a Privacy Policy Office, it should take care that any such office does not promulgate top-down privacy rules and regulations. An office created solely to oversee privacy policy, and with a mandate to create "codes" and "best practices"—even voluntary ones—could, unless properly supervised and restrained, develop into an agency that sees its role as creating new rules and codes, often based on abstract or theoretical concerns, which may not be compatible with empirical practices and practical needs.

ABM further notes that, as the Report states, the FTC is and will remain the lead consumer privacy enforcement agency of the U.S. Government. (Report, p. 51.) Thus, it is not clear how a Privacy Policy Office within the Commerce Department would function within a privacy oversight or regulatory framework, given that the FTC will continue to have significant authority in this area.

ABM supports the suggestions that if a Privacy Policy office is created, it should work closely with industry experts such as chief privacy officers, and leverage their expertise. (Report, p. 49.) Indeed, ABM believes the listening function of the office is so important that the office's first objectives should be to listen to industry experts concerning current industry practices and voluntary codes, in addition to those who are seeking to change or impose new requirements on business. There should be no mandate that the office work toward creation of new codes or best practices guidelines if they are not needed, and in order to determine needs, the office should first survey the current landscape, working closely with industry officials like chief privacy officers.

ABM agrees that education of consumers is very important, and that Commerce and its proposed Privacy Policy Office could take a leadership role in this regard. Indeed ABM believes that many of the concerns raised by various groups about consumer misunderstandings are not caused by inadequate privacy protections, but by consumer misunderstandings, or lack of understanding, of the procedures and protections that are available to them and the benefits they ring to users. If consumers more fully understand the options they already have, and the options that are becoming available to them under programs such as the advertising industry self-regulation program for online behavioral advertising, they may well find these existing programs adequate and effective to protect their privacy interests while serving their desires to participate fully in e-commerce. Thus, a full and effective educational campaign may help avoid the need for new rules and regulations.

Commerce Issue #6: Global Privacy Harmonization

ABM agrees that the Department should continue its work on an international data privacy framework. ABM agrees with the Report that differences between U.S. and other national privacy laws make it increasingly complicated for companies to provide goods and services in global markets, and that "the U.S. Government should work with our allies and trading partners to promote low-friction, cross-border data flow through increased global interoperability of privacy frameworks." (Report, p. 7.) Indeed, ABM believes that such efforts should be one of Commerce's top priorities with respect to data privacy, and that the Department has the experience and expertise needed in this area.

ABM notes, however, that the need for global interoperability should not be taken as an imperative to conform U.S. laws to the much more restrictive, and less business- and innovation-friendly approaches, of some nations and alliances, such as that of the European Union. Rather, methods should be developed that respect and preserve U.S. laws and practices, including the recognition that business entities and individuals who act on their behalf do not have personal privacy rights in their business activities. As the report notes, the department must take care "to prevent conflicting policy regimes from serving as trade barriers." (Report, p. 20.)

Thank you for your consideration of these comments.

Sincerely,
THOMPSON COBURN LLP

By 
Mark Sableman

Attorneys for American Business Media

cc: Mr. Clark Pettit